REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application. Applicants would also like to thank the Examiner for the courtesies extended during the telephone interview on November 14, 2006.

The arguments discussed during the Examiner's interview are now presented in the current response, and are as follows: 1) generation of a same secret key by both the central processing unit and the peripheral device, and 2) the transmission line is connected directly between the central processing unit and the peripheral device.

To advance prosecution of the present case, the claim recitation "a transmission line connected in parallel with said data bus between said at least one peripheral device and said central processing unit" has been changed back to "a transmission line connected between said at least one peripheral device and said central processing unit." This recitation was in the claims as initially examined by the Examiner. In other words, the "parallel" claim recitation added in the Amendment filed May 23, 2006 has been removed. Consequently, the 35 U.S.C. 112 rejection should be withdrawn.

The claim amendments and arguments supporting patentability of the claims are presented in detail below.

I. The Claimed Invention

The present invention, as recited in amended independent Claim 12, for example, is directed to an electronic

device comprising a central processing unit, at least one peripheral device, and a data bus connected between the at least one peripheral device and the central processing unit through which data travels at a rate of a clock signal.
The electronic device further comprises a transmission line connected between the at least one peripheral device and the central processing unit for providing a random signal thereto that is synchronous with the clock signal. The central processing unit and the at least one peripheral device each comprises a data encryption/decryption cell connected to the data bus and to the transmission line for generating a same current secret key at each clock cycle based upon the random signal.

The data encryption/decryption cell in the central processing unit and in the at least one peripheral device advantageously makes the electronic device more secure by making it more difficult to determine the data elements that travel through the data bus when an intruder observes current consumption of the electronic device.

Amended independent device Claim 25 is similar to amended independent device Claim 12 except the at least one peripheral device has been changed to at least one memory device. Amended independent device Claim 34 is similar to amended independent device Claim 12 except this claim is directed to a smart card. Amended independent method Claim 42 is similar to amended independent device Claim 12.

II. The Claims Are Patentable

The Examiner rejected independent Claims 12, 25, 34 and 42 over the Miyazaki et al. patent. The Examiner has taken the position that the claimed invention is disclosed in columns 7 through 9 of the Miyazaki et al. patent. The text in columns 7 through 9 corresponds to the block diagram of an IC card **101**. The IC card **101** comprises a CPU **102**, a ROM **103**, an EEPROM **104**, an I/O port **105** for controlling input/output to/from the IC card, a RAM **106**, and a residual multiplier **107**. The components are interconnected through a bus **108**.

During the Examiner's interview, the Examiner explained that he had taken the position that the EEPROM **104** in the Miyazaki et al. patent generates a secret key **d** at each clock cycle based upon the random signal **k**; and that the IC card **101** itself is the peripheral device which also generates a secret key at each clock cycle based upon the random signal **k** as in the claimed invention. The Examiner appears to have taken this position in part because of the abstract disclosing that "... the IC card incorporates residual multiplier hardware for implementing a high-speed algorithm for a residual multiplication arithmetic, a method and a device capable of executing a public key encryption processing such as an elliptic curve encryption processing at a high speed."

The Examiner is correct to note that the EEPROM **104** generates a secret key **d**. The secret key **d** is discussed in column 9, line 5 and column 10, lines 8-14. The Miyazaki et al. patent

only discloses that the secret key **d** is stored in the EEPROM **104**.

The Miyazaki et al. patent fails to disclose that the secret key **d** is also stored in any of the peripheral devices such as ROM **103** and RAM **106**, for example. Consequently, since the Miyazaki et al. patent fails to disclose generation of a secret key **d** by a peripheral device other than the EEPROM **104**, then the Miyazaki et al. patent also fails to disclose a peripheral device comprising a data encryption/decryption cell for generating the secret key **d** as in the claimed invention.

The Applicants submit that even though the IC card **101** in the Miyazaki et al. patent is capable of performing encryption/decryption algorithms, this is with respect to the EEPROM **104**. Anyone of the peripheral devices within the IC card **101** itself is not generating a secret key **d**.

The Applicants submit that the Miyazaki et al. patent does not deal with the encryption of the transmissions between the CPU and the peripherals, since the value "aR mod p" is not encrypted for transmission between the EEPROM **104** and the multiplier **107**. (Column 9, lines 35-50). In other words, values of elliptic points calculated by the EEPROM **104** are not encrypted for their transmission on the bus **108** between the EEPROM **104** and the multiplier **107**.

The Miyazaki et al. patent thus fails to provide any protection for data transmitted on the bus **108**. In sharp contrast, the data encryption/decryption cell in the central processing unit and in the at least one peripheral device advantageously makes the electronic device more secure by making

it more difficult to determine the data elements that travel through the data bus when an intruder observes current consumption of the electronic device.

Secondly, the Miyazaki et al. patent fails to disclose that the secret key **d** is generated based upon a random signal that is synchronous with the clock signal as in the claimed invention. The Miyazaki et al. patent discloses a random number **k**, but fails to disclose that the random number is used to generate the secret key **d**. Instead, the random number **k** is stored in the EEPROM **104** and is used in the "calculation **k*P**, i.e., multiplication of the base point **P** on the elliptic curve by the random number **k**." (Column 9, lines 45-50). The bit string **k** is discussed in greater detail in column 10, lines 38-55, but no reference is made to generation of the secret key **d**.

In addition, during the Examiner's interview, the Examiner characterized I/O line **114** as the transmission line, and since this line is connected to the I/O port **105**, the transmission line is then connected to the CPU **102** and the peripheral devices. However, the Applicants submit that this interpretation of the Miyazaki et al. patent is not supported in the detailed description. The transmission line **114** may only connected to the CPU **102**, for example. The Miyazaki et al. patent thus fails to clearly disclose that a transmission line is connected between the CPU **102** and any of the peripheral devices on the IC card **101** for providing a random signal thereto that is synchronous with the clock signal, as in the claimed invention.

Accordingly, it is submitted that amended independent Claim 12 is patentable over the Miyazaki et al. patent. Amended independent Claims 25, 34 and 42 are similar to amended independent Claim 12. It is submitted that these independent claims are also patentable over the Miyazaki et al. patent. In view of the patentability of the amended independent Claims 12, 25, 34 and 42, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the amendments to the claims and the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330